COMPLEX MULTIPLICATION: LECTURE 11/12

1. Algebraic curves

Recall we are interested in studying the solutions to the equation

$$y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

Now we have developed enough of the language of algebraic geometry in order to make sense of this object. This is an affine algebraic set given by the vanishing of the above polynomial in $\mathbb{A}^2_{\mathbb{C}}$, thus it is an algebraic variety of dimension 1. However we are really more interested in the studying the projectivistion of this curve, so adding the extra variable z, we obtain the homogenous equation:

$$ZY^2 = 4X^3 - g_2(\tau)XZ^2 - g_3(\tau)Z^3$$

This is a projective variety obtained by adding the point $(0 : 1 : 0)$. We will show later on that this variety is in fact non-singular, this motivates the following definition.

Definition 1.1. In this course, a curve over a perfect field k is a non-singular projective algebraic variety over k of dimension 1.

The following section will cover the theory of algebraic curves that we will need to discuss the theory of elliptic curves over a general field.

Remark 1.2. When $k = \mathbb{C}$, curves (in our sense) are just compact Riemann surfaces, so if you have studied Riemann surfaces before, a lot of the following results should be quite familiar.

Let C be a curve, we write $\overline{k}(C)$ for the function field of C, and if P is a point on C, we let $\overline{k}[C]_P$ be the local ring at P. The first important result is the following

Proposition 1.3. *$\overline{k}[C]_P$ is a a discrete valuation ring.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of $\overline{k}[C]_P$, then by definition $\mathfrak{m}/\mathfrak{m}^2$ is a 1 dimensional vector space. Then since $\overline{k}[C]_P$ is Noetherian, this follows from [AM] Prop 9.2. □

A local parameter t at the point P is a uniformizer of the DVR $\overline{k}[C]_P$.

Note however that the above is false if C is not smooth.

Example 1.4. Let C be the curve defined by $y^2 = x^3$ in $\mathbb{A}^2_{\overline{k}}$. Then the maximal ideal $\mathfrak{m}$ of the local ring at 0 has $\dim_{\overline{k}} \mathfrak{m}/\mathfrak{m}^2 = 2$, hence $\mathfrak{m}$ cannot be principle.

Let $f \in \overline{k}(C)$ be a non-zero rational function and let t be a local parameter at P. Then since $\mathrm{Frac}(\overline{k}[C]_p) = \overline{k}(C)$, it follows that there exists $n \in \mathbb{Z}$ such that $t^n f \in \overline{k}[C]_P^\times$. We define

$$\mathrm{ord}_P(f) = n$$

the order of f at p. Since

$$\mathrm{ord}_P f/g = \mathrm{ord}_P f - \mathrm{ord}_P g$$

we obtain a homomorphism $\overline{k}(C)^\times \to \mathbb{Z}$. By convention we let $\mathrm{ord}_P 0 = \infty$ so we can extend the above to a map

$$\overline{k}(C) \to \mathbb{Z} \cup \infty$$

Definition 1.5. We say f is regular, resp. has a zero, resp. has a pole at P if $\mathrm{ord}_P(f) \geq 0$ resp. $\mathrm{ord}_P(f) > 0$, resp. $\mathrm{ord}_P(f) < 0$). If f is regular at P then we can evaluate f at P to get $f(P) \in \overline{k}$.

The following is the analogue of a familar theorem in the theory of Rieman surfaces.

Proposition 1.6. *Let $f \in \overline{k}[C]_P$, then f has finitely many zeros/poles. If f is regular then $f \in \overline{k}$.*

Proof. Beyond the scope of this course. The idea is to consider f as a function from C to $\mathbb{P}^1$, and to prove the algebraic analogue of the theorem in Riemann surfaces that the sum of the preimages of any point counted with multiplicity is equal to a number n independend of the point. □

Exercise: Let C be the curve $y^2 = x^3 + x$. We checked this was nonsingular last time. Let P be the point $(0, 0)$.

i) Show that $\mathfrak{m}_P/\mathfrak{m}_P^2$ is generated by y, hence y is uniformizer at P.

ii) Compute $\mathrm{ord}_P(x)$.

We now discuss morphisms between curves, the following property is very special to smooth curves.

Proposition 1.7. *Let $\phi : C_1 \to V$ be a rational map where $V \subset \mathbb{P}^n$ is a projective variety. Then for any point $P \in C_1$, f is regular at P and hence f is a regular map.*

Proof. By definition f is given by a tuple $(g_0 : ... : g_n)$ where the $g_i \in \overline{k}(C)$. Let $P \in C$ and let t be a local parameter at P, then let

$$m = \min_i(\mathrm{ord}_P(g_i))$$

Then ϕ is also given by

$$(t^{-m}g_0 : ... : t^{-m}g_n)$$

which by definition of m is regular at P. □

We also need to following theorem whose proof is beyond the scope of this course.

Proposition 1.8. *Let $\phi : C_1 \to C_2$ be a morphism of curves, then ϕ is either surjective or constant.*

Remark 1.9. This is analogous to the property that a holmorphic map between Rieman surfaces is either constant or surjective. The point is that projectivity is the algebraic analogue of compactness, so that the image of such morphism will be closed. Here we mean closed in the Zariski topology, we have not defined this yet but for curves the closed sets are just points. The result then follows by noting that C_1 is connected and a morphism of varieties is necessarily continuous for the Zariski topology.

The results above allow us to deduce that algebraic curves have a rather simple description using their fraction fields. Let C_1 and C_2 be curves over k and let $\phi : C_1 \to C_2$ be a morphism of curves defined over k. Then if ϕ is non-constant, we obtain a homorphism of function fields $\phi^* : k(C_2) \to k(C_1)$. The main result is then the following.

Theorem 1.10. *The association $C \mapsto k(C)$ gives a bijection between isomorhpism classes of algebraic curves over k and field extensions K/k of transcendence degree 1 such that $K \cap \overline{k} = \emptyset$. The association $\phi \mapsto \phi^*$ induces a correspondence between non-constant morphisms of algebraic curves defined over k and field injections fixing k.*

Remark 1.11. For people familiar with category, this just says that the category of algebraic curves and non-constant morphisms between them is equivalence to the opposite category of fields k' as above and injections between them.

This theorem is implied by the following proposition.

Proposition 1.12. *Let C_1 and C_2 be curves.*

i) Let $\phi : C_1 \to C_2$ be a non-constant morphism defined over k, then $k(C_1)/\phi^* k(C_2)$ is a finite extension.

ii) Let $i : k(C_2) \to k(C_1)$ be an inclusion of fields, then there exists a unique $\phi : C_1 \to C_2$ such that $\phi^* = i$

iii) Let K/k be a field of transcendence degree 1 over k such that $K \cap \overline{k} = k$, then there exists an algebraic curve C defined over k such that $k(C) = K$.

Proof. i) $k(C_1)$ and $k(C_2)$ both have transdence degree 1 over k, hence $k(C_1)/\phi^* k(C_2)$ is an algebraic extension, but $k(C_2)$ is finitely generated over k hence the extension is finite.

ii) Let $C_2 \subset \mathbb{P}^n$ and wlog. assume C is not contained in the hyperplane cute out by X_0. For $i = 1, ..., n$ let $g_i \in k(C_2)$ be the rational function corresponding to X_i/X_0 on C_2. Then

$$\phi := (1 : ig_1 : ... : ig_n)$$

is a rational map between C_1 and C_2 which satisfies $\phi^* = i$. Then ϕ is not constant since not all the g_i are constant, otherwise C_2 would just be a point.

If $\psi = (f_0 : ... : f_n)$ was another rational map such that $\psi^* = i$, then

$$f_i/f_0 = \psi^* g_i = \phi^* g_i = ig_i$$

hence $\psi = \phi$.

iii) See Hartshorne for the proof of the algebraically closed case. Given K, the idea is to look at all the set C of valuations of K, this should correspond to the points of K. Let $U \subset C$ be a subset such that $C \backslash U$ is finite, then one defines $k[U] = \bigcap_{p \in U} R_p$ where R_p is the valuation ring of p. One shows that this $k[U]$ is the coordinate ring of an affine curve whose points correspond precisely to U. $\square$

Exercise: Let $k = \overline{k}$, recall a valuation on $K = k((t))$ is a function $v : K^\times \to \mathbb{Z}$ such that

i) $v(ab) = v(a) + v(b)$

ii) $v(a + b) \geq \min(v(a), v(b))$

a) Let $a \in \overline{k}$, and for $f \in K$ let $f(t) = (t-a)^n \frac{g(t)}{h(t)}$ where $t - a \nmid g(t), h(t)$. Define $v_a(f) = n$, show that v_a is a valuation on k.

b) Let $f = \frac{g(t)}{h(t)}$ and let $n = \deg g, m = \deg h$. Define $v_\infty(f) = m - n$, show that v_∞ is a valuation on K.

c) Let v be a valuation on K such that $v(k^\times) = 0$, prove that v is of the form v_a for some $a \in k \cup \infty$.

d) Let $R_a \subset K$ be the valuation ring corresponding to v_a. Show that $\cap_{a\in k} R_a = k[t]$.

This allows us to define the structure of an affine algebraic variety on the set $\{v_a : a \in k\}$, whose ring of regular functions is $\cap_{a\in k} R_a = k[t]$, so that the resulting variety is just $\mathbb{A}^1$. We can repeat this procedure to get a cover of the set of valuations of K. One can check that the resulting variety is isomorphic to $\mathbb{P}^1$.

Definition 1.13. Let $\phi : C_1 \to C_2$ be a morphisms of curves. We define the degree $\deg \phi$ of ϕ to be 0 if ϕ is constant and the integer $[k(C_1) : \phi^* k(C_2)]$ otherwise.

In the setting of compact Riemann surfaces, one usually defines the degree of a map ϕ to be the number of preimages of a point $P \in C_2$ counted with multiplicity which one shows is independent of the point. That this is correct algebraic analogue follows from the next result.

Given $\phi : C_1 \to C_2$ be a map of curves, let $Q \in C_1$ and let t be a uniformiser of the local ring at $\phi(Q)$. Then $\phi^* t \in \overline{k}(C_1)$ and we let $e_Q = \mathrm{ord}_Q(\phi^* t)$, this is the *ramificaiton index* at Q.

Proposition 1.14. *Let $\phi : C_1 \to C_2$ be a morphism of degree n. For $P \in C_2$, let $\phi^{-1}(P) = \{Q_1, ..., Q_k\}$, then we have*

$$\sum_{i=1}^{k} e_{Q_i} = n$$

Proof. See [Hartshorne] II 6.9 □

Corollary 1.15. *Let $\phi : C_1 \to C_2$ be a morphism of elliptic curves, if $\deg \phi = 1$, then ϕ is an isomorphism.*

Proof. As $\deg \phi = 1$, ϕ^* is an isomorphism of fields, hence there exists an inverse $\psi^* : k(C_1) \to k(C_2)$. This corresponds to a rational map $\psi : C_2 \to C_1$ which by **??** is a morphism of curves. Then since $\psi^*\phi^*$ and $\phi^*\psi^*$ are the identity maps, it follows that $\phi\psi$ and $\psi\phi$ are the identity. □

1.1. **The Frobenius map.** Suppose now that $\mathrm{char}(k) = p > 0$ and let $q = p^r$. For any $f \in k[x_1, ..., x_n]$, $f = \sum_I a_I X^I$ where $I = (i_1, ..., i_n) \in \mathbb{Z}^n$ and X^I denotes $x_1^{i_1} ... x_n^{i_n}$, we define a new element $f^{(q)}$ by raising all the coefficients of f to the q^{th} power, i.e.

$$f^{(q)} = \sum_I a_I^q X^I$$

Let $C \subset \mathbb{P}^n$ be an algebraic curve and let I be the homogenous ideal corresponding to V. Then we define a new ideal

$$I^{(q)} = \text{ideal generated by} \{f^{(q)} : f \in I\}$$

$I^{(q)}$ is homogeneous and we let $C^{(q)}$ be the variety defined by $I^{(q)}$.

Remark 1.16. The construction $C^{(q)}$ is independent of the embedding into $\mathbb{P}^n$, since if $C \subset \mathbb{P}^m$ is another embedding and $\phi = (f_0 : ... : f_m) : \mathbb{P}^n \to \mathbb{P}^m$ inducing an isomorphism between the embedded curves, then raising the coefficients of the f_i to the q^{th} power gives an isomorphism between the embedded $C^{(q)}$'s.

Example 1.17. Let C in $\mathbb{P}^2$ be the curve defined

$$ZY^2 = X^3 + aXZ^2 + bZ^3$$

then $C^{(q)}$ is defined by

$$ZY^2 = X^3 + a^qXZ^2 + b^qZ^3$$

There is a natural map $\phi : C \to C^{(q)}$ which is given by

$$\phi : (x_0 : ... : x_n) \mapsto (x_0^q : ... : x_n^q)$$

If f vanishes on x, the clearly $f^{(q)}$ vanishes on $\phi(x)$, so this is well defined.

Definition 1.18. We call ϕ the q^{th} power Frobenius map.

Recall a field extension L/K is called separable if the minimal polynomial of any $\alpha \in L$ over K is a power of $(X - a)$.

Definition 1.19. We say a map of curves $\phi : C_1 \to C_2$ (defined over k) is separable (resp. inseparable resp. purely inseparable) if the corresponding extension of function fields $k(C_1)/\phi^*k(C_2)$ has that property.

Proposition 1.20. *Let k be a field of characteristic $p > 0$, C a curve defined over k and $\phi : C \to C^{(q)}$ the q^{th} power frobenius map.*
a) $\phi^*k(C^{(q)}) = k(C)^q = \{f^q : f \in k(C)\}$.
b) ϕ purely inseparable of degree q.

Proof. a) Recall the desciption given by Yihang of the function field $k(C)$; its elements are given by quotients f/g where f and g are homogeneous polynomials of the same degree. Then $\phi^*(f/g) = f(x_0^q, ..., x_n^q)/g(x_0^q, ..., x_n^q)$, but on the other hand $K(C)^q$ consists of polynomials of the form f^q/g^q. But since we assumed k was perfect any polynomial $f(x_0^q, ..., x_n^q)$ is a q^{th} power of the polynomial whose coefficients are the q^{th} roots of the coefficisntaof f, hence $\phi^*f/g \in \overline{k}(C)^q$. Conversely any polynomial which is a q^{th} power is of the form $f(x_0^q, ..., x_n^q)$ so we obtain the reverse inclusion, thus the two fields coincide.

b) The fact that the extension is purely inseparable follows immediately from part a). To prove that the degree is q, let $t \in k(C)$ be a uniformiser at any point P. We need the following Lemma.

Lemma 1.21. The field extension $k(C)$ is a finite separable extension of $k(t)$.

Proof of **??**. t cannot be algebraic over k since if $\sum_{i=0}^n a_it^i = 0$, wlog. we can assume $a_0 \neq 0$, then

$$1 \leq \text{ord}_P \sum_{i=1}^n a_it^i = \text{ord}_P a_0 = 0$$

Thus since $k(C)$ is finintely generated of transcendence degree 1 over k, $k(C)$ is a finite extension of $k(t)$.

Thus for $x \in k(C)$, x has a minimal polynomial Φ over $k(t)$. In fact $\Phi(T, X)$ be the polynomial in two variables such that $\Phi(t, X)$ is the minimal polynomial of X. Then if x is not separable, we must have

$$\Phi(T, X) = \Psi(T, X^p)$$

for some other polynomial Ψ.

We want to construct a polynomial of smaller degree in X for which x is a root, thus contradicting the minimality of Φ. Let

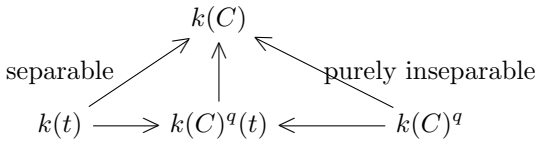
$$\Phi(T, X) = \sum_{i,j} a_{ij} T^i X^{jp}$$

and let $b_{ij} = a_{ij}^{1/p}$ which exists since we assumed k was perfect. Then grouping together the terms for which i is the same mod p, we obtain:

$$\begin{aligned}\Phi(T, X) &= \sum_{k=0}^{p-1} \sum_{i,j} (b^p_{(i+k)j} T^{ip} X^{jp}) T^k \\ &= \sum_{k=0}^{p-1} \sum_{i,j} (b_{(i+k)j} T^i X^j)^p T^k \\ &= \sum_{k=0}^{p-1} \Phi_k(T, X)^p T^k\end{aligned}$$

Now if evaluate at (t, x), then the order of vanishing at P of $\Phi_k(T, X)T^k$ is distinct mod$p$. Hence if some $\Phi_k(t, x)^p$ is non-zero, the expression vanishes to finite order at P so cannot be 0. Thus $\Phi_k(t, x)^p = 0$ for all k and hence $\Phi_k(t, x) = 0$ for all k. Then some $\Phi_k(T, X)$ must have a term involving X, then $\Phi_k(t, x) = 0$ contradicting minimality of Φ. □

We have the tower of fields



Thus the extension $k(C)/k(C)^q(t)$ is both separable and purely inseparable, hence $k(C) = k(C)^q(t)$, so we need to show $k(C)^q(t)/k(C)^q$ has degree q. Since $t^q \in k(C)^q(t)$, we only need to check $t^{q/p}$ is not in $k(C)^q$, but t is a uniformiser at O, so that $t^{q/p}$ would have non-integral valuation at p otherwise. □